**IT Security and Risk Management**

**December 2023 Examination**

**1. As a term, people, process, and technology (PPT) refers to the methodology in which the balance of people, process, and technology drives action: People perform a specific type of work for an organization using processes (and often, technology) to streamline and improve these processes. What do you mean by security awareness for people, process, and technology? (10 Marks)**

**Ans 1.**

**Introduction:**

In the realm of IT security and risk management, the triad of people, process, and technology (PPT) forms the backbone of an organization's security posture. While each component of this triad is distinct, they are deeply interwoven, with the effectiveness of one often depending on the other two. Security awareness, in this context, is not just about understanding threats and vulnerabilities but also about cultivating a proactive mindset towards safeguarding assets. It emphasizes the importance of each element in the PPT triad being cognizant of, and resilient against, potential security threats. By fostering

It is only half solved

Buy Complete from our online store

<https://nmimsassignment.com/online-buy-2/>

NMIMS Fully solved assignment available for**session December 2023,**

your**last date is 29th November 2023**.

Lowest price guarantee with quality.

Charges**INR 299 only per assignment.**For more information you can get via mail or Whats app also

Mail id is aapkieducation@gmail.com

Our website [www.aapkieducation.com](http://www.aapkieducation.com/)

After mail, we will reply you instant or maximum

1 hour.

Otherwise you can also contact on our

whatsapp no 8791490301.

Contact no is +91 87-55555-879

**2. Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data. Companies often grant access to information and assets to staff even if it is not relevant to that member of staff’s role. Describe access control methodologies and implementation for purpose of security? Give detailed justifications for your recommendations. (10 Marks)**

**Ans 2.**

**Introduction**

Access control is a foundational pillar of information security, ensuring that only authorized individuals can access specific resources within an organization. It operates on the principle of "least privilege," which means granting users only the permissions they need to perform their job functions. In the digital age, where data breaches and cyberattacks are rampant, implementing robust access control mechanisms is not just a best practice but a necessity. Without proper access controls, organizations risk exposing sensitive data to unauthorized

**3. Bangladesh Bank is the central bank of Bangladesh, responsible for managing the country's monetary and financial stability. In February 2016, cybercriminals launched a sophisticated attack on the bank's foreign exchange reserves, attempting to steal hundreds of millions of dollars.**

**Incident Details:**

**SWIFT Transactions: The attackers used the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network to initiate fraudulent fund transfers. They sent multiple payment requests to the Federal Reserve Bank of New York, requesting the transfer of approximately $951 million from Bangladesh Bank's account to various accounts in the Philippines and Sri Lanka.**

**Authentication Bypass: The cybercriminals managed to compromise the bank's SWIFT terminal and gain access to the SWIFT system using stolen credentials. They were able to manipulate SWIFT messages to make the transactions appear legitimate.**

**Errors Detected: A few of the fraudulent transfer requests contained spelling errors that raised suspicions at the Federal Reserve Bank. This prompted further scrutiny. Prevented Losses: While the attackers successfully transferred $81 million to the Philippines, an alert official at the Federal Reserve Bank noticed the spelling errors in subsequent transfer requests. This raised suspicions and led to the cancellation of several transactions, preventing further losses.**

**Investigation: After the attack was discovered, Bangladesh Bank launched an investigation and sought assistance from law enforcement agencies and cybersecurity experts.**

**Consequences:**

**Bangladesh Bank lost approximately $81 million in the successful transactions.**

**The incident raised concerns about the security of the global financial system and the vulnerabilities in SWIFT's infrastructure.**

**It also highlighted the importance of cybersecurity for financial institutions worldwide. Attribution:**

**While the cybercriminals responsible for the Bangladesh Bank heist were never conclusively identified, there have been suspicions that North Korean hackers, specifically the Lazarus Group, were involved due to similarities with other attacks attributed to them.**

**a. In the Bangladesh Bank Cyber Heist case, what were the key vulnerabilities and security lapses that allowed the cybercriminals to compromise the bank's systems and attempt a fraudulent transfer of funds? Provide specific examples from the case to support your answer. (5 Marks)**

**Ans 3a.**

**Introduction**

The Bangladesh Bank Cyber Heist of 2016 stands as a stark reminder of the vulnerabilities that even major financial institutions can face in the realm of cybersecurity. The incident underscores the importance of robust security measures, especially when dealing with global financial systems. The attackers exploited a combination of technical vulnerabilities and operational lapses to attempt one of the largest bank heists in history. This case serves as a

**b. Discuss the role of international cooperation and information sharing in responding to cyber attacks on financial institutions, as illustrated by the Bangladesh Bank Cyber Heist. What lessons can be drawn from this case regarding the importance of cross-border cooperation in cybersecurity? (5 Marks)**

**Ans 3b.**

**Introduction**

The digital age has ushered in an era where cyber threats transcend national borders, making international cooperation and information sharing paramount. The Bangladesh Bank Cyber Heist serves as a prime example of how cyber attacks on financial institutions can have global ramifications. In such a landscape, a siloed approach to cybersecurity is inadequate. Instead, a